February 23, 2018

E Street Communications, Inc.
96 Inverness Dr E Ste: G
Englewood, CO 80112
tel: 303-584-0640 fax: 303-584-0652
web: http://www.estreet.com
e-mail: support@estreet.com

** Operating Procedures **

E STREET COMMUNICATIONS, INC.
OPERATING PROCEDURES & POLICIES

Overall Statement: E Street, Inc. and its affiliates utilize reasonable and adequate safeguards and procedures to protect Customer Proprietary Network Information, including but not limited to: 1) employee training; 2) following "opt-out" notice rules; 3) electronic flagging of customer accounts; 4) password protection of account information; 5) seeking authorization and permission from customers prior to accessing customer information; and 6) adhering to internal compliance policies relating to customer privacy and information. Also, neither E Street Communications, Inc. nor its affiliates sell customer information to outside firms or vendors.

Specific Procedures: E Street takes very seriously its obligation to safeguard CPNI from unauthorized access by employees and agents. As a result, we currently have the following specific procedures in place to ensure that we are in compliance with the rules in 47 C.F.R. Section 64:

1) The company follows FCC rules relating to opt-out or opt-in notification provisions for its customers.
2) The Company requires the use of secure logins and verifications against security flags within our database to control access to data. E Street agents must sign an Agency Agreement that deems our customer information as proprietary to E Street, and states that they are bound by the same rules as our employees to keep such information confidential.
3) Beginning with the employee job application, E Street communicates to its employees the importance of protecting the confidentiality of all company-related information, including CPNI. During employee training and orientation, E Street's Human Resources department trains each employee on privacy and security of customer information and the employee is provided a handbook that contains E Street's policies on confidentiality of information.
4) The company has conducted a comprehensive CPNI training session for senior management employees.
5) Privacy of customer information is reinforced among E Street employees with special employee bulletins delivered via email, and documents contained on the company Intranet. In short, all employees having access to customer account information receive specialized training on when it is permissible to use, disclose or permit access to CPNI.
6) The company has established provisions in its Corporate Compliance Program Procedures for dealing with potential unauthorized employee/agent breaches that could result in disciplinary action or criminal or civil liability. E Street would also alert and work with the appropriate law enforcement agency to resolve the offense.
7) To detect external (third party) breaches that may occur, E Street utilizes Network Intrusion and Detection equipment which places network sensors at internet entry points into our internal networks. These sensors monitor incoming network traffic and generate real-time alerts 24 hours a day. Also, firewall devices are placed between un-trusted and trusted networks. These limit and restrict network traffic to only what is necessary for business purposes in a secure manner. Firewall logs are monitored for unusual and suspicious activity.
8) E Street's password management policy is known to E Street employees working with CPNI. For online access to CPNI, each time a customer and/or an employee attempts to log-in, authentication is required. E Street's procedures also limit the number of unsuccessful password/authentication attempts. After five unsuccessful attempts to enter a password, the involved account can be either suspended until reset by a system administrator, or temporarily disabled for no less than 15 minutes.

9) A CPNI privacy flag, which contains the employee id and name, is attached to each account at the time the account is viewed. Additionally, E Street validates employee access to systems which contain Subscriber Account Information. Employee access is granted based upon the employee's job functions and duties and direct authorization of the owner. If an employee changes jobs or departs from the company, his access can be revoked by the owner and further security instructions can be flagged to the account. Also, E Street monitors calls and provides training on when customer approval is required before subscriber account information can be accessed.
10) E Street has developed a written CPNI policy on account confidentiality which sets forth company policy on using, disclosing or giving access to information regarding customers' accounts.
11) E Street has a specific company policy related to critical or sensitive data. This policy is posted on the company's internal website accessible to all employees. It states, inter alia, that confidential information and other Company information that is not for public viewing must not be sent through email, must not be sent over the Internet, and must not be posted to any mailing list, newsgroup or other public area. This includes, but is not limited to, such items as CPNI and customer account passwords. The company's policy goes on to say that auto-forwarding of email to accounts outside the organization is not permitted. E Street will take disciplinary action, up to and including termination, against any employee found to have violated these policies.
12) E Street ensures any customer information saved or downloaded to a laptop computer is password protected. To further reduce the likelihood of unauthorized access on remote computers E Street takes steps to NOT maintain and store any live customer information on remote computers at any time with the exception of customer accounts within our data center.